100.2412
Branigan 2-10

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants:	Branigan et al.
Serial No.:	09/755,470
Filed:	January 5, 2001
For:	METHODS AND APPARATUS FOR SECURE WIRELESS NETWORKING
Group:	2134
Examiner:	Tran, Ellen C.

Durham, North Carolina
April 28, 2005

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Declaration of Lowell Ross Pursuant to 37 C.F.R. 1.131

Dear Sir:

I, Lowell W. Ross, Jr., declare as follows:

1. All statements herein made of my own knowledge are true and all statements made on my information and belief is believed to be true.

2. On information and belief, the present application has been rejected under 35 U.S.C. 102(e) as anticipated by Hagen U.S. Patent Application Publication No. 2002/0075844 (Hagen) having a publication date of June 20, 2002, a filing date of April 10, 2001, and potentially claiming priority of a provisional application filed December 15, 2000.

3. As outlined in greater detail below, the invention as claimed in our present application was conceived before December 15, 2000 by the inventors, Mr. Branigan and Mr. Cheswick, and was diligently reduced to practice constructively by the preparation and filing of the present application on January 5, 2001.

4. I was at the time in question and am currently an employee of the Law Offices of Peter H. Priest, P.L.L.C. ("the firm") and I principally prepared the present application.

5. On December 1, 2000, I faxed a draft of the present application to Peter Priest, the senior partner in the firm. Later that day, I received a marked up draft of the present application containing comments from Peter Priest. A true copy of the marked up draft of the present application proving conception of present invention prior to December 15, 2000 is attached as Exhibit A hereto.

6. I worked on making the edits suggested by that markup and I sent an email to the lead inventor on December 6, 2000 requesting clarification of acronyms used in an attached draft of the present application. The version of the draft in the attachment contains incorporated comments received from Peter Priest on December 1, 2000. A true copy of the email is attached as Exhibit B hereto.

7. On information and belief, I made further edits to the draft of the present application on December 13, 2000. A true copy of this version of the present application further proving conception of present invention prior to December 15, 2000 is attached as Exhibit C hereto.

8. From before December 15. 2000 until the filing date of January 5, 2001, I worked diligently with the lead inventor and others within the firm to finalize the application for filing.

9. I received a composite email on December 20. 2000 which includes the lead inventor's response to my email requesting clarification of acronyms used in the draft of the present application. A true copy of the composite email I received on December 20, 2000 is attached as Exhibit D hereto.

10. The law firm was closed for the holidays during the work week beginning December 25. 2000 until January 2. 2001.

11. The present application. Serial No. 09/755,470. was filed January 5. 2001.

12. The acts outlined above which are relied upon to establish a date prior to the Hagen publication were carried out in the United States.

I declare under penalty of perjury under the laws of the Untied States of America that the foregoing is true and correct. I understand that willful false statements and the like are punishable by fine or imprisonment or both as set forth in 18 U.S.C. 1001. and may jeopardize the validity of the application or any patent issuing thereon.

Executed on April 28, 2005

Lowell W. Ross, Jr.
Lowell W. Ross, Jr., Esq.

12-1-00

EXHIBIT A

METHODS AND APPARATUS FOR SECURE WIRELESS NETWORKING

Field of the Invention

The present invention relates generally to improvements in wireless network security. More particularly, the invention relates to the use of a wireless network to connect wireless clients to a wired network using an authenticating server which authenticates users for connection to the wired network.

Background of the Invention

Wireless data networking is becoming more popular as wireless data transfer rates continue to increase. Wireless networking presents great convenience for users in allowing them to connect to the network without having to limit their mobility by the need to have access to a wired connection. The data transfer performance provided by present day wireless communication devices is acceptable for many applications and the increased speeds which can be expected as new devices are developed will make wireless connections suitable for more and more applications. As developing technology allows greater transfer rates, the increased transfer rates, combined with the inherent convenience and ease of use of a wireless connection, will greatly increase the prevalence of wireless networks.

However, wireless networking presents security problems which are not typically found in wired networks. Physical access to a wired network can be controlled by controlling access to the wires connected to the network. Every network connection point can be physically identified and can be controlled and monitored, and the extent of the network can be precisely known by mapping the wiring and connection points. It is much more difficult to control access to a wireless network. Connections to a wireless network occur across three dimensional space and the precise boundaries within which an acceptable wireless connection can be made are difficult to identify. Defining the boundaries within which eavesdropping can occur is even more difficult, because an eavesdropper does not need a perfect transmission and need not necessarily understand all data transmitted in order to gain enough information to seriously compromise confidential data. Wireless networking hardware providers attempt to address the security issues through constructs which limit access to the wireless network or provide security through end to end encryption. A typical prior art wireless network employs a plurality of wireless base stations, each using a single encryption key to secure transmissions to and from clients communicating with that base station. All users communicating with a base station must share the encryption key used by the base station. This presents security problems as users leave the network. In order to maintain good security, all keys which may be known to a user need to be changed whenever a user leaves a network. In the case of a shared key, this requires that all client devices which used the previous key be provided with the new key. Moreover, users of a wireless network are likely to move between base stations. Wireless networking is intended to provide mobility and convenience for users, and a network covering a significant area and employing a number of base stations is likely to be designed to provide connectivity to users without regard to their location, and without requiring them to be within range of a single designated base station in order to establish a connection.

Because a user can communicate with more than one base station, the user needs to have encryption keys for each base station for which a connection is to be established. If a user attempts to connect to a base station and does not have a key for that base station, the connection will fail. It is not convenient for a user to have a connection rejected because he or she moves from a first base station to a second base station without having a key for the second base station. In order to prevent such situations, wireless networks often use one key for all base stations, with the key shared by all users. When the network is first deployed, this arrangement provides acceptable security, but as users leave the system security tends to degrade. Good security practices require that all keys and passwords known to a user be changed whenever that user leaves the network, but it is difficult to enforce this practice if it means that new keys must be generated and distributed to all users on the network whenever a user leaves the system. Maintaining different keys for each base station does not solve the problem, particularly if all users may use all base stations at different times. In that case, each user must be provided with the key used by each base station, and when a user leaves the network, each base station's key must be changed and the new keys must be distributed to all users. Commonly, keys are not changed and as time passes the population of potential unauthorized users possessing encryption keys becomes larger and larger.

Furthermore, wireless network passwords tend to be few in number and shared by all users or a large group of users. Sharing of passwords presents many of the same problems as does sharing of encryption keys.

Moreover, wireless data networking components may themselves be subject to attack. Wireless data networking is relatively new and the encryption techniques employed by wireless data networks have not yet been tested as thoroughly as those used by wired networks. Unknown weaknesses may therefore exist in the encryption used by a particular wireless networking component or group of components.

There exists, therefore, a need for a system which allows wireless networking which provides known, reliable security techniques to prevent eavesdropping and other compromises of system integrity, and which which employs authentication and security protocols which allow each user to be assigned a unique password and encryption key each having a status independent of the passwords and encryption keys of other users.

Summary of the Invention

Among its several aspects,
~~A~~ a network according to the present invention includes a wireless network providing connectivity to client stations with improved security. Depending on design, the wireless network comprises a single wireless access point or alternatively a plurality of wireless access points connected to a central hub. The wireless network provides communication between the wireless access points and the client stations, but does not perform any authentication to control connection to the wireless access points. The wireless network access point is assigned an address on a wired network and provides a connection to an SB server which controls access to the wired network by clients on the wireless network. The SB server is typically connected to a network hub on the wired network and acts as a gateway to wired network resources for clients on the wireless network. When a wireless network client establishes a connection to the SB, the SB server performs authentication for the wireless network client, typically by authenticating the username and password of the wireless network client using a user database. Once the wireless network client has been authenticated, the SB server provides the wireless network client with a temporary Internet protocol (IP) address on the wired network, using DHCP. The SB server also provides the wireless network client with a unique session key to be used for encrypted communication with the wired network. The session key is used by one client during one connection session to the wired network.

spell out

It is not necessary to control access to the wireless network because the wireless network in and of itself does not provide access to anything of value. The wireless network only provides access to the SB server, which will not provide access to wired network resources without authentication and which, moreover, encrypts all information passed to the wireless network. Without authentication, a wireless network client cannot gain access to wired network resources and an eavesdropper cannot gain access to network information because all traffic over the wireless network which contains substantive information from the wired network is encrypted.

A more complete understanding of the present invention, as well as further features and advantages of the invention, will be apparent from the following Detailed Description and the accompanying drawings.

Brief Description of the Drawings

Fig. 1 illustrates a connection between a wireless network and a wired network according to the present invention, with authentication of wireless network users and control of access to the wired network performed by a server according to the present invention, with the wireless network providing a single wireless access point for connection by wireless clients;

Fig. 2 illustrates a connection between a wired network and a wireless network employing connection, encryption and authentication techniques according to the present invention, the wireless network comprising multiple wireless access points; and

Fig. 3 illustrates a process of network authentication and security according to the present invention.

Detailed Description

Fig. 1 illustrates a wired network 100 which provides authentication and security to wireless ? network clients according to the present invention. The wired network 100 includes an SB server 102 according to the present invention, providing a connection between the wired network 100 and a wireless network 104. The SB server 102 controls access to the wired network 100 by the wireless network 104, and provides address and authentication services to clients of the wireless network 104. The wired network 100 also preferably comprises a network hub 106, which provides a connection to additional wired network resources including, but not limited to a user authentication database 108 for use by the SB server 102 in authenticating clients seeking access to the wired network 100 and a DHCP server 110 for providing temporary addresses to authenticated clients of the wired network 100.

The wireless network 104 comprises a wireless network access point 112 providing wireless network connections to network client devices such as laptop computers 114A. . .114N, each of the computers 114A. . .114N connecting to the access point 112 using a wireless network card 116A. . .116N, respectively. The wireless network access point 112 and the wireless network cards 116A. . .116N preferably support 128-bit encryption in order to provide secure communication between wireless network clients and the SB server 102. In the implementation shown here, the wireless network cards are WAVELAN cards conforming to the IEEE/802.11 networking standard and the client devices 114A. . .114N have installed point to point tunneling protocol (PPTP) software supporting 128-bit encryption. The use of particular networking cards and the use of PPTP, however, are not essential features of the present invention, and many other implementations may be envisioned, including the use of the LUCENT Virtual Private Network (VPN) Gateway in place of PPTP, or the use~~d~~ of SSH in place of PPTP. The use of SSH allows use of the present invention in a UNIX/X-Windows environment.

The wireless network access point 112 is assigned a permanent address on the wired network 102 in order to allow the wireless devices 114A. . .114N to connect to the SB server 102 to request authentication for access to the wired network 102. Similarly, the SB server 102 is assigned a permanent address on the wireless network 104 in order to provide routing from the wireless network 104 to the wired network 100.

When a user of a device, for example a user of the computer 114A, wishes to connect to the wired network 100 using the wireless network 104, ~~the user makes~~ a connection to the wireless access point 112 is established using the wireless network card 116A. Connection and address information for the wireless network 104 can be widely published and disseminated, because the wireless network 104 does not provide access to any resources other than the ability to request the SB server 102 to provide authentication and access to the wired network 100. Initial traffic between the client computer 114A and the wireless SB server 102 is encrypted, using encryption protocols supported by the SB server 102 and the wireless network card 116A. This is done because the client computer 114A will send confidential information such as a username and password to the access point 112 in order to request the SB server 102 to provide authentication and it is important to protect this information from eavesdroppers. Encryption of traffic passing between the computer 114A and the access point 112 may suitably be accomplished using public key cryptography, which makes unnecessary the transferring of secret keys between the client computer 114A and the SB server 102. The wireless network access point 112 does not need to encrypt any data, because encryption and decryption occur at the SB server 102 and the wireless network card 116A card during initial authentication and at the SB server 102 and the wireless network client 114A once authentication has been accomplished.

Once the client computer 114A has been connected to the wireless network access point 112, the access point 112 transfers information between the computer 114A and the SB server 102 using the network protocol employed by the wired network 102 and the wireless network 104. The network protocol used is preferably a virtual private network protocol, and in the exemplary implementation illustrated here is point to point tunneling protocol. A virtual private network is a configuration which allows the use of publicly available facilities to be used to establish a connection between entities (such as clients and servers) which are part of a private network. Virtual private network protocols provide security between entities belonging to the private network, in order to prevent eavesdropping or other compromise of information or resources by persons who have access to the public facilities but who are not authorized users of the private network. An example of a virtual private networking arrangement would be the use by a corporation of the Internet to connect remote network users to the central corporate network. In the exemplary case illustrated here, the use of the wireless network 104 to connect clients to the wired network 100 is a case of virtual private networking, even if the wireless network 104 is provided and maintained by the owner or administrator operating the wired network 100. This is because the wireless network 104 is publicly accessible, in that no effort is made to restrict its use, even if it is not specifically developed as a resource to be offered to the general public. Therefore, virtual private network protocols such as point to point tunneling protocol, are used to protect the information traveling over the wireless network 104, so that security is managed by entities involved in the connection to the wired network 100, such as the client computer 114A, network card 116A and SB server 102, without any need for the wireless network 104 to contribute to maintaining security.

Once the client computer 114A establishes a connection to the SB server 102, the SB server 102 performs authentication. Authentication is preferably performed using the authentication system implemented in Plan 9 from Bell Laboratories, but may suitably be performed according to any desired authentication system, providing that the system provides proper security. The SB server 102 preferably logs each connection attempt, whether or not the connection attempt was successful, in order to allow for later auditing and security analysis. The SB server requests authentication information, typically a username and password. The user provides the username and password, which is transmitted wirelessly to the access point 112 and then communicated to the SB server 102 using a wired connection between the access point 112 and the SB server 100. Once the SB server 102 receives the authentication information, it compares the authentication information against the information contained in the user authentication database 108. If the authentication information received from the client computer 114A does not match the information in the database 108, the SB server 102 rejects the connection attempt. Preferably, the SB server 102 provides the user with a predetermined number of attempts to provide correct authentication information and then, if an excessive number of attempts is

Anything to incorporate by Ref. ?

made, imposes a delay before a new attempt will be processed. This procedure helps to protect against repeated automated attempts to guess authentication information. The SB server 102 preferably logs each authentication attempt and does not provide any access to resources on the wired network 102 until valid authentication information is received. When valid authentication information is received, the SB server 102 requests an IP address from a DHCP server 110 and furnishes this address to the client computer 114A. The SB server 102 also secures subsequent communications with the client computer 114A, preferably using the Microsoft implementation of RC-4, but may suitably use any desired system for providing communication security. The SB server 102 furnishes an encryption key to the client computer 114A for cryptoprocessing information transferred between the client computer 114A and the SB server 102. Once the key has been furnished to the client computer 114A, it is not necessary for the wireless access point 112 to perform encryption, because encryption is already being performed by the SB server 102 and the client computer 114A, and neither will transmit plaintext information to the other during the remainder of the session. Once authentication has been performed and the client computer 114A has been given an address for access to thc wired network, the client computer 114A is allowed access to network resources according to the privileges associated with the username used in authentication.

It is also possible to employ an SB server to provide connection to a wireless network comprising a plurality of wireless network access points. Fig. 2 illustrates a wired network 200 employing an SB server 202 to provide authentication and security for wireless clients according to the present invention. The wired network 200 also includes a wired network hub 204 and various additional nctwork resources a user databasc 206 and a DHCP server 208. Thc SB scrver 202 provides connection services to allow clients connected to a wireless network 210 to gain access to network resources using the same protocols described above in connection with Fig. 1.

The wired network 210 comprises two wireless access points 212 and 214 connected to a network hub 216, which is in turn connected to the SB server 202. The wireless access point 212 is connected to a client computer 218 by means of a wireless network card 220 and the wireless access point 214 is connected to a client computer 222 by means of a wireless network card 224. For simplicity, the wireless network 210 is shown here as comprising two wireless access points, each connected to a single client computer. However, it will be recognized that the wireless network 210 may include any number of wireless access points, each connected to a plurality of client computers, with the only limitation on the number of wireless access points and the number of client computers connected to each access point being those suggested by sound network management practices. Authentication and communication security are preferably performed as described above in connection with the SB server 102 of Fig. 1.

The use of an SB server to control access to a wired network by a wireless network provides good scaling for any size of wireless network. The number of connections to the wired network scales arithmetically as the size of the wireless network increases, with no more than one connection to the SB server being presented with each addition of a wireless access point to the wireless network. Moreover, the management of passwords and keys is not increased in complexity by the addition of wireless access points. When a user leaves a network such as the wired network 200, his or her authorization to use the wired network 200 can be removed at the user database 206, without any need to make changes at any of the wireless network access points such as the access points 214 and 216 in the case of the wireless network 210, or potentially many more access points in the case of a larger network.

Because the radio footprint of a wireless network such as the network 210 is unknown, it must be assumed that an attacker may have access to the radio transmissions used to transfer data between the elements of the network. The attacker may be able to eavesdrop on wireless network sessions, hijack a session by impersonating a client computer with an already established connection to the network, interrupt a session or initiate a session. However, because the wireless network 210 contains no information or access to resources having value to an attacker, the vulnerability of the wireless network is unimportant. Because thc wired network 200 is protected by the SB server 202, which implements a well tested authentication system and uses strong encryption to pass data to the wireless network 210, the vulnerability of the wireless network 210 does not compromise any data or resources in the wired network 200. Traffic analysis of the clients and encrypted sessions are available to an eavesdropper, because the communications are radiated over a footprint of unknown size. However, the use of PPTP encapsulates the network traffic, causing all traffic to have an address tuple of the client system and the SB server 202. Traffic analysis, therefore, will not yield the addresses of the SB server and the client computers such as the computer 218.

Fig. 3 illustrates a process 300 of authenticating and securing a connection between a wireless network client and a wired network according to the present invention. At step 302, a connection is established between a wired network and a wireless network. The wireless network may suitably be similar to the wireless network 104 of Fig. 1 and the wired network may suitably be similar to the wired network 100 of Fig. 1. Connection may suitably be established between the wired network and the wireless network by establishing a connection between an SB server similar to the SB server 102 of Fig. 1 and a wireless network access point similar to the access point 118 of Fig. 1. At stcp 304, a connection is established bctwccn a wireless network client and thc wirelcss network, suitably by establishing a connection between the wireless network client and the wireless network access point. The wireless network client may suitably be similar to the computer 114A of Fig. 1, and may suitably communicate with the access point with a wireless network card similar to the network card 116A of Fig. 1. At step 305, in response to a request to establish a connection between the wireless network client and the wired network, encryption keys are exchanged between the wireless network client and the server in order to protect data to be used for authentication. Next, at step 306, authentication is performed for the wireless network client, suitably by requesting and receiving a username and password and comparing the username and password against a user database. The information exchanged between the server and the client is encrypted using the keys exchanged at step 305. If authentication fails, the process proceeds to step 350, the connection is rejected and the connection attempt is logged. If authentication passes, the process proceeds to step 308 and the connection attempt is logged. Next, at step 312, the wireless network client is provided with a temporary address on the wired network, preferably using DHCP, and a unique session encryption key for use in communicating with the wired network. At step 314, traffic is passed between the wireless network client and the wired network through the SB server, with access to network resources being given to the client in accordance with the user privileges associated with the account information provided for authentication.

in a secure manner ?

While the present invention is disclosed in the context of a presently preferred embodiment, it will be recognized that a wide variety of implementations may be employed by persons of ordinary skill in the art consistent with the above discussion and the claims which follow below.

We claim:

1. A wired network for providing secure, authenticated access to wireless network clients, comprising:

a server connected to a wireless network access point, the server being operative to perform authentication for wireless clients establishing a connection to the server through the wireless network access point, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client, the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client; and

a user database accessible to the server for use in validating wireless clients.

2. The wired network according to claim 1 and also including a network hub providing connections between the server and additional resources on the wired network.

3. The wired network according to claim 2 wherein the server is operative to provide addresses to clients through dynamic host control protocol.

4. The wired network according to claim 3 wherein the server is operative to communicate with the wireless network access point using point to point tunneling protocol.

5. The wired network according to claim 4 wherein the server employs 128-bit cryptoprocessing to communicate with the wireless network access point.

6. A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:

a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network, the wireless network access point being operative to conduct encrypted communications with the server, the wireless network access point being further operative to receive authentication information from clients and transfer the authentication information to the server and to receive a cryptoprocessing key from the server and transfer the key to each of the clients; and

a plurality of wireless network clients operative to establish connections with the wireless network access point, each client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point and receive address information and cryptoprocessing data from the network access point to allow communication with the wired network, each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information.

7. The wireless network of claim 6 wherein the access point communicates with the server using point to point tunneling protocol.

8. The wireless network of claim 7, also including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and the additional network access points being operative to establish connections with the server through the network hub.

9. A method of secure communication between wireless network clients and a wired network, comprising the steps of:

Think about some more method claims

establishing a connection between an SB server connected to the wired network and a wireless network access point;

establishing a connection between the SB server and a network client communicating with the SB server through the wireless network access point;

exchanging encryption keys between the SB server and the wireless network client;

performing authentication for the wireless network client;

if authentication fails, rejecting connection to the wired network; and

if authentication passes, accepting connection to the wired network, providing a temporary wired network address and a unique session encryption key to the wireless network client and providing access to wired network resources in response to requests by the wireless network client.

10. The method of claim 9 wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection and wherein the step of accepting the connection is accompanied by a step of logging the acceptance.

What about
session
limited
access

ABSTRACT

Techniques for secure connections between wireless network clients and wired network resources are described. An insecure wireless network comprising a plurality of wireless access points provides a connection for wireless network clients to a wired network server which in turn provides controlled access to a wired network. When a wireless network user wishes to connect to the wired network, the user provides authentication information to the wired network server through the wireless network client and the wireless network access point. Once the wired network server has verified the authentication information, the wired network server provides the wireless network client with a temporary wired network address as well as a unique session encryption key, which is used to encrypt all data transferred between the wireless network client and the wired network server during a connection session.

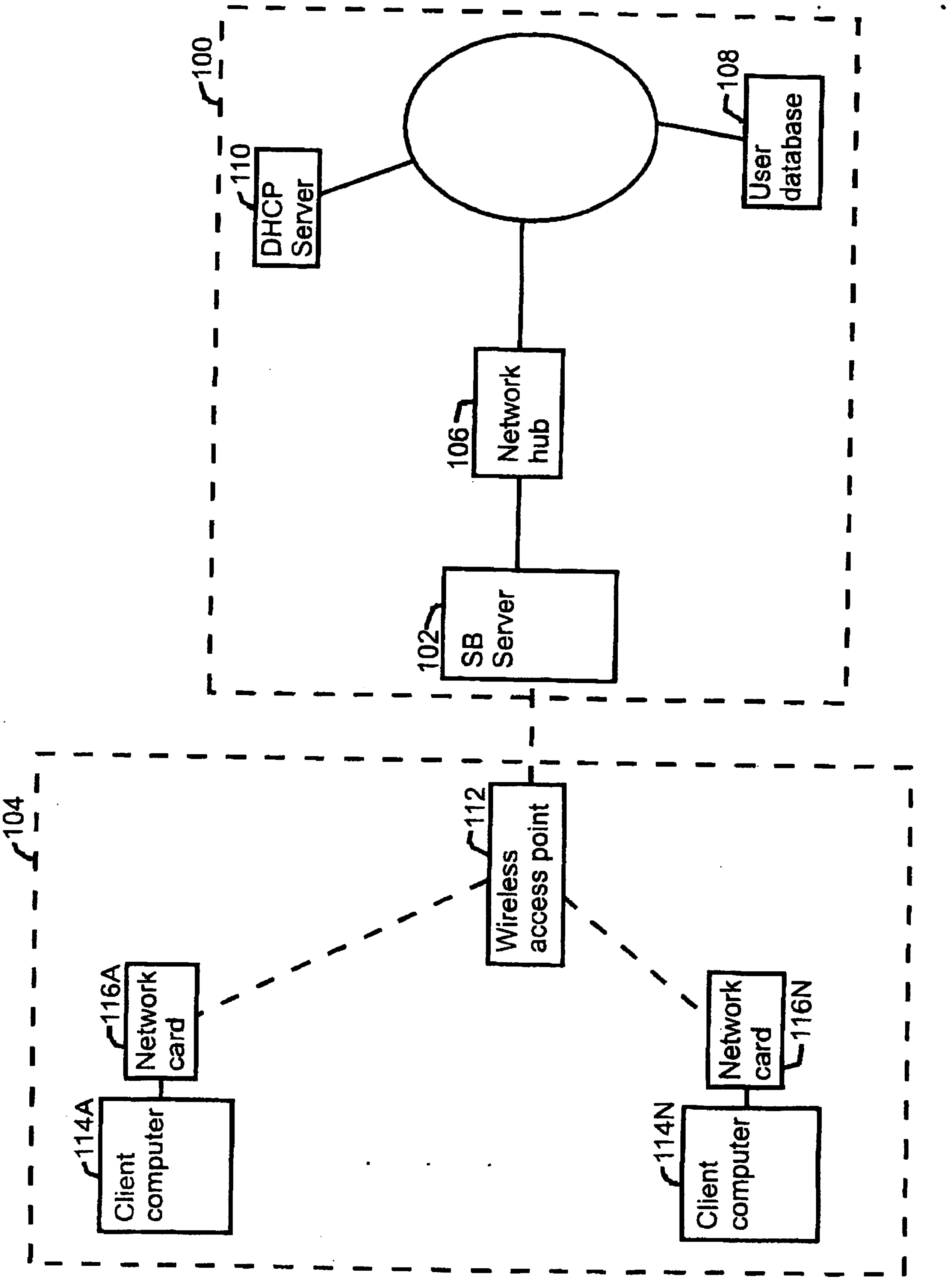
100
110
DHCP Server
108
User database
106
Network hub
102
SB Server
104
112
Wireless access point
116A
Network card
114A
Client computer
116N
Network card
114N
Client computer

Fig. 1

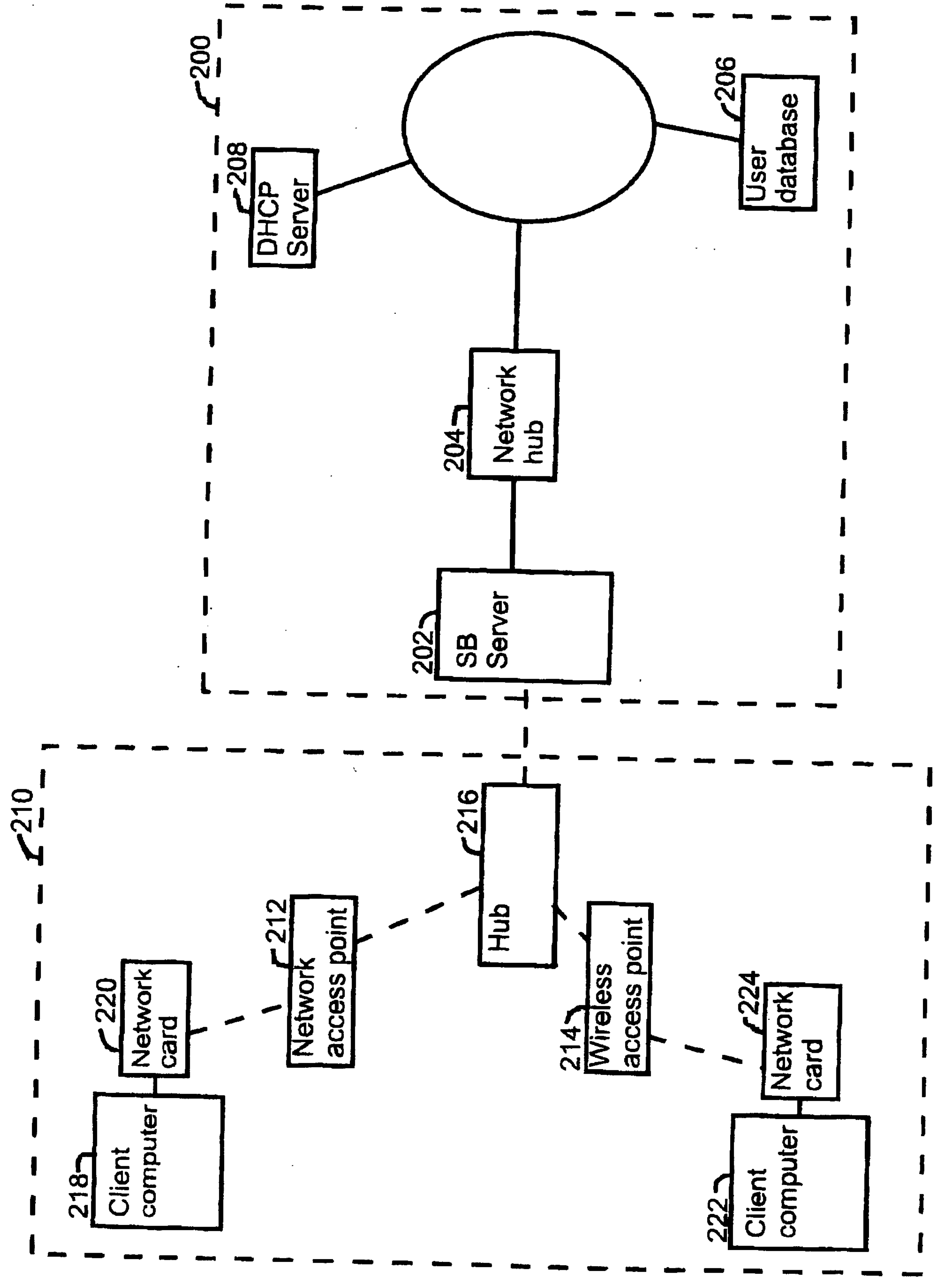
200
208
DHCP Server
206
User database
204
Network hub
202
SB Server
210
216
Hub
212
Network access point
214
Wireless access point
220
Network card
224
Network card
218
Client computer
222
Client computer

Fig. 2

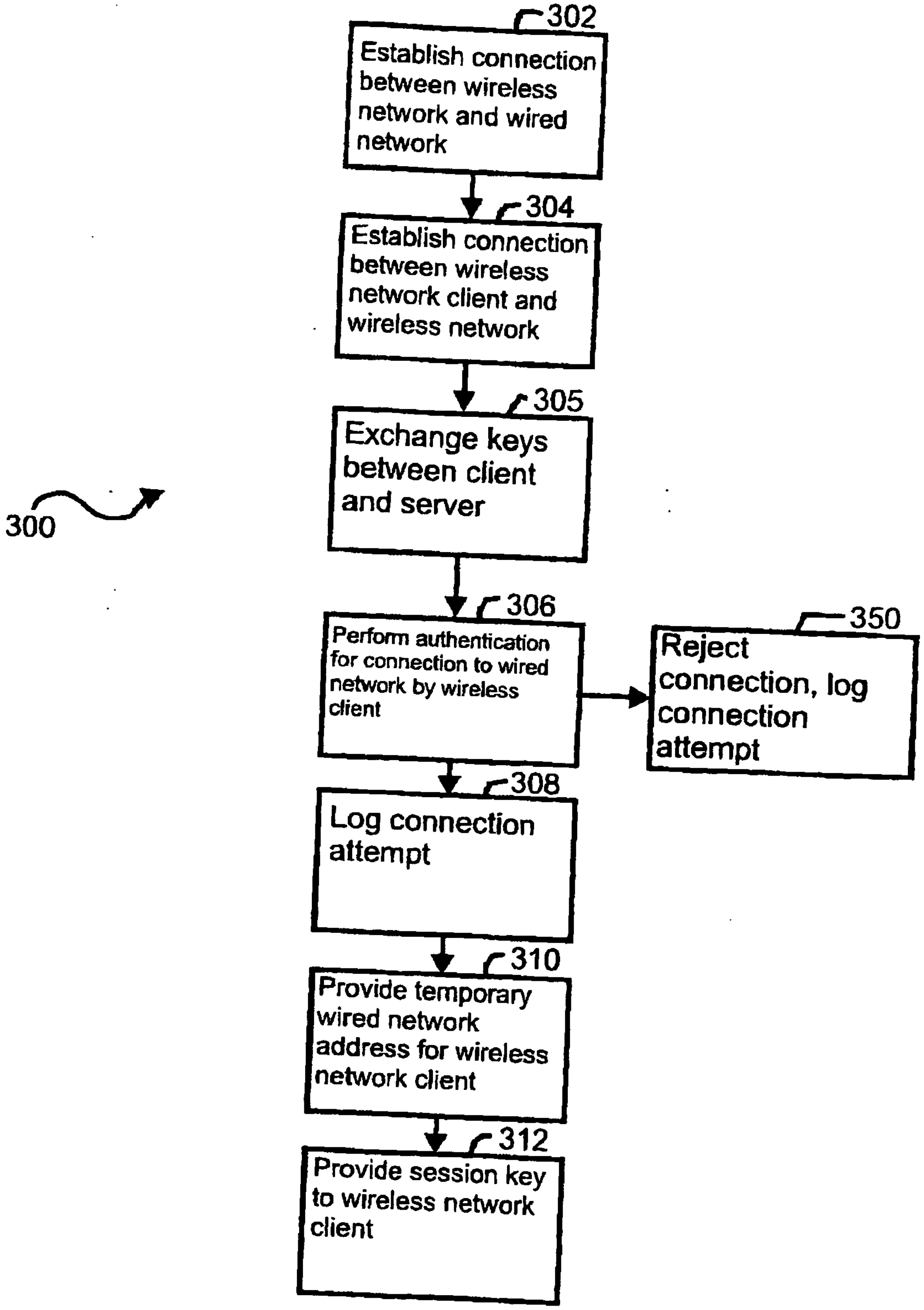
302
Establish connection between wireless network and wired network
304
Establish connection between wireless network client and wireless network
305
Exchange keys between client and server
300
306
Perform authentication for connection to wired network by wireless client
350
Reject connection, log connection attempt
308
Log connection attempt
310
Provide temporary wired network address for wireless network client
312
Provide session key to wireless network client

Fig. 3

Vickie Prior

EXHIBIT B

From: "Lowell Ross" <lowellross@mediaone.net>
To: "steve branigan" <sb@lumeta.com>
Sent: Wednesday, December 06, 2000 3:27 PM
Attach: IDS 121218.zip.pgp; Lowell Ross 2.asc
Subject: Re: my key!

Hi, Steve, here is the document, along with my key.

I want to make sure that all the abbreviations are defined. I believe the only ones I didn't spell out are SB for SB server, and SSH, in the discussion of possible alternative implementations, but there may be more.

Thanks!

Lowell
(714)979-0576
(Not admitteed in California)

#3 12-13-00

2412

EXHIBIT C

METHODS AND APPARATUS FOR SECURE WIRELESS NETWORKING

Field of the Invention

The present invention relates generally to improvements in wireless network security. More particularly, the invention relates to the use of a wireless network to connect wireless clients to a wired network using an authenticating server which authenticates users for connection to the wired network.

Background of the Invention

Wireless data networking is becoming more popular as wireless data transfer rates continue to increase. Wireless networking presents great convenience for users in allowing them to connect to the network without having to limit their mobility by the need to have access to a wired connection. The data transfer performance provided by present day wireless communication devices is acceptable for many applications and the increased speeds which can be expected as new devices are developed will make wireless connections suitable for more and more applications. As developing technology allows greater transfer rates, the increased transfer rates, combined with the inherent convenience and ease of use of a wireless connection, will greatly increase the prevalence of wireless networks.

However, wireless networking presents security problems which are not typically found in wired networks. Physical access to a wired network can be controlled by controlling access to the wires connected to the network. Every network connection point can be physically identified and can be controlled and monitored, and the extent of the network can be precisely known by mapping the wiring and connection points. It is much more difficult to control access to a wireless network. Connections to a wireless network occur across three dimensional space and the precise boundaries within which an acceptable wireless connection can be made are difficult to identify. Defining the boundaries within which eavesdropping can occur is even more difficult, because an eavesdropper does not need a perfect transmission and need not necessarily understand all data transmitted in order to gain enough information to seriously compromise confidential data. Wireless networking hardware providers attempt to address the security issues through constructs which limit access to the wireless network or provide security through end to end encryption. A typical prior art wireless network employs a plurality of wireless base stations, each using a single encryption key to secure transmissions to and from clients communicating with that base station. All users communicating with a base station must share the encryption key used by the base station. This presents security problems as users leave the network. In order to maintain good security, all keys which may be known to a user need to be changed whenever a user leaves a network. In the case of a shared key, this requires that all client devices which used the previous key be provided with the new key. Moreover, users of a wireless network are likely to move between base stations. Wireless networking is intended to provide mobility and convenience for users, and a network covering a significant area and employing a number of base stations is likely to be designed to provide connectivity to users without regard to their location, and without requiring them to be within range of a single designated base station in order to establish a connection.

Because a user can communicate with more than one base station, the user needs to have encryption keys for each base station for which a connection is to be established. If a user attempts to connect to a base station and does not have a key for that base station, the connection will fail. It is not convenient for a user to have a connection rejected because he or she moves from a first base station to a second base station without having a key for the second base station. In order to prevent such situations, wireless networks often use one key for all base stations, with the key shared by all users. When the network is first deployed, this arrangement provides acceptable security, but as users leave the system security tends to degrade. Good security practices require that all keys and passwords known to a user be changed whenever that user leaves the network, but it is difficult to enforce this practice if it means that new keys must be generated and distributed to all users on the network whenever a user leaves the system. Maintaining different keys for each base station does not solve the problem, particularly if all users may use all base stations at different times. In that case, each user must be provided with the key used by each base station, and when a user leaves the network, each base station's key must be changed and the new keys must be distributed to all users. Commonly, keys are not changed and as time passes the population of potential unauthorized users possessing encryption keys becomes larger and larger.

Furthermore, wireless network passwords tend to be few in number and shared by all users or a large group of users. Sharing of passwords presents many of the same problems as does sharing of encryption keys.

Moreover, wireless data networking components may themselves be subject to attack. Wireless data networking is relatively new and the encryption techniques employed by wireless data networks have not yet been tested as thoroughly as those used by wired networks. Unknown weaknesses may therefore exist in the encryption used by a particular wireless networking component or group of components.

There exists, therefore, a need for a system which allows wireless networking which provides known, reliable security techniques to prevent eavesdropping and other compromises of system integrity, and which employs authentication and security protocols which allow each user to be assigned a unique password and encryption key each having a status independent of the passwords and encryption keys of other users.

Summary of the Invention

Among its several aspects, a network according to the present invention includes a wireless network providing connectivity to client stations with improved security. Depending on design, the wireless network comprises a single wireless access point or alternatively a plurality of wireless access points connected to a central hub. The wireless network provides communication between the wireless access points and the client stations, but does not perform any authentication to control connection to the wireless access points. The wireless network access point provides a connection to an SB server which controls access to the wired network by clients on the wireless network. The SB server has an interface attached to the wireless network. The interface to the wireless network has an address on the wired network. The SB server is typically connected to a network hub on the wired network and acts as a gateway to wired network resources for clients on the wireless network. When a wireless network client establishes a connection to the SB, the SB server performs authentication for the wireless network client, typically by authenticating the username and password of the wireless network client using a user database. Once the wireless network client has been authenticated, the SB server provides the wireless network client with a temporary (Internet protocol) IP address on the wired network, using dynamic host control processing (DHCP). The SB server also provides the wireless network client with a unique session key to be used for encrypted communication with the wired network. The session key is used by one client during one connection session to the wired network.

It is not necessary to control access to the wireless network because the wireless network in and of itself does not provide access to anything of value. The wireless network only provides access to the SB server, which will not provide access to wired network resources without authentication and which, moreover, encrypts all information passed to the wireless network. Without authentication, a wireless network client cannot gain access to wired network resources and an eavesdropper cannot gain access to network information because all traffic over the wireless network which contains substantive information from the wired network is encrypted.

A more complete understanding of the present invention, as well as further features and advantages of the invention, will be apparent from the following Detailed Description and the accompanying drawings.

Brief Description of the Drawings

Fig. 1 illustrates a connection between a wireless network and a wired network according to the present invention, with authentication of wireless network users and control of access to the wired network performed by a server according to the present invention, with the wireless network providing a single wireless access point for connection by wireless clients;

Fig. 2 illustrates a connection between a wired network and a wireless network employing connection, encryption and authentication techniques according to the present invention, the wireless network comprising multiple wireless access points; and

Fig. 3 illustrates a process of network authentication and security according to the present invention.

Detailed Description

Fig. 1 illustrates a wired network 100 which provides authentication and security to wireless network clients according to the present invention. The wired network 100 includes an

SB server 102 according to the present invention, providing a connection between the wired network 100 and a wireless network 104. The SB server 102 controls access to the wired network 100 by the wireless network 104, and provides address and authentication services to clients of the wireless network 104. The wired network 100 also preferably comprises a network hub or router 106, which provides a connection to additional wired network resources including, but not limited to a user authentication database 108 for use by the SB server 102 in authenticating clients seeking access to the wired network 100 and a DHCP server 110 for providing temporary addresses to authenticated clients of the wired network 100.

The wireless network 104 comprises a wireless network access point 112 providing wireless network connections to network client devices such as laptop computers 114A...114N, each of the computers 114A...114N connecting to the access point 112 using a wireless network card 116A...116N, respectively. [The wireless network cards 116A...116N may suitably support 128-bit encryption in order to provide secure communication between wireless network clients and the SB server 102.] In the implementation shown here, the wireless network cards are WAVELAN cards conforming to the IEEE/802.11 networking standard and the client devices 114A...114N have installed point to point tunneling protocol (PPTP) software supporting 128-bit encryption. The use of particular networking cards and the use of PPTP, however, are not essential features of the present invention, and many other implementations may be envisioned, including the use of the LUCENT Virtual Private Network (VPN) Gateway in place of PPTP, or the use of SSH in place of PPTP. The use of SSH allows use of the present invention in a UNIX/X-Windows environment.

The SB server 102 is assigned a permanent address on the wireless network 104 in order to allow the wireless devices 114A...114N to connect to the SB server 102 to request authentication for access to the wired network 100. Similarly, the SB server 102 is assigned a permanent address on the wired network 100 in order to provide routing from the wireless network 104 to the wired network 100.

When a user of a device, for example a user of the computer 114A, wishes to connect to the wired network 100 using the wireless network 104, a connection to the wireless access point 112 is established using the wireless network card 116A. Connection and address information for the wireless network 104 can be widely published and disseminated, because the wireless network 104 does not provide access to any resources other than the ability to request the SB server 102 to provide authentication and access to the wired network 100. Initial traffic between the client computer 114A and the wireless SB server 102 is encrypted, using encryption protocols supported by the SB server 102 and the wireless network card 116A. This is done because the client computer 114A will send confidential information such as a username and password to the access point 112 in order to request the SB server 102 to provide authentication and it is important to protect this information from eavesdroppers. Encryption of traffic passing between the computer 114A and the access point 112 may suitably be accomplished using public key cryptography, which makes unnecessary the transferring of secret keys between the client computer 114A and the SB server 102. The wireless network access point 112 does not need to encrypt any data, because encryption and decryption occur at the SB server 102 and the wireless network card 116A card during initial authentication and at the SB server 102 and the wireless network client 114A once authentication has been accomplished.

Once the client computer 114A has been connected to the wireless network access point 112, the access point 112 transfers information between the computer 114A and the SB server 102 using the network protocol employed by the wired network 102 and the wireless network

104. The network protocol used is preferably a virtual private network protocol, and in the exemplary implementation illustrated here is point to point tunneling protocol. A virtual private network is a configuration which allows the use of publicly available facilities to be used to establish a connection between entities (such as clients and servers) which are part of a private network. Virtual private network protocols provide security between entities belonging to the private network, in order to prevent eavesdropping or other compromise of information or resources by persons who have access to the public facilities but who are not authorized users of the private network. An example of a virtual private networking arrangement would be the use by a corporation of the Internet to connect remote network users to the central corporate network. In the exemplary case illustrated here, the use of the wireless network 104 to connect clients to the wired network 100 is a case of virtual private networking, even if the wireless network 104 is provided and maintained by the owner or administrator operating the wired network 100. This is because the wireless network 104 is publicly accessible, in that no effort is made to restrict its use, even if it is not specifically developed as a resource to be offered to the general public. Therefore, virtual private network protocols such as point to point tunneling protocol, are used to protect the information traveling over the wireless network 104, so that security is managed by entities involved in the connection to the wired network 100, such as the client computer 114A, network card 116A and SB server 102, without any need for the wireless network 104 to contribute to maintaining security.

Once the client computer 114A establishes a connection to the SB server 102, the SB server 102 performs authentication. Authentication is preferably performed using the authentication system implemented in Plan 9 from Bell Laboratories, but may suitably be performed according to any desired authentication system, providing that the system provides proper security. The SB server 102 preferably logs each connection attempt, whether or not the connection attempt was successful, in order to allow for later auditing and security analysis. The SB server requests authentication information, typically a username and password. The user provides the username and password, which is transmitted wirelessly to the access point 112 and then communicated to the SB server 102 using a wired connection between the access point 112 and the SB server 100. Once the SB server 102 receives the authentication information, it makes a connection to the user authentication database 108 using the wired network 100 and compares the authentication information received from the client computer 114A against the information contained in the user authentication database 108. If the authentication information received from the client computer 114A does not match the information in the database 108, the SB server 102 rejects the connection attempt. Preferably, the SB server 102 provides the user with a predetermined number of attempts to provide correct authentication information and then, if an excessive number of attempts is made, imposes a delay before a new attempt will be processed. This procedure helps to protect against repeated automated attempts to guess authentication information. The SB server 102 preferably logs each authentication attempt and does not provide any access to resources on the wired network 102 until valid authentication information is received. When valid authentication information is received, the SB server 102 requests an IP address from a DHCP server 110 and furnishes this address to the client computer 114A. The SB server 102 also secures subsequent communications with the client computer 114A, preferably using the Microsoft implementation of RC-4, but may suitably use any desired system for providing communication security. The SB server 102 furnishes an encryption key to the client computer 114A for cryptoprocessing information transferred between the client computer 114A and the SB server 102. Once the key has been furnished to the client computer 114A, it is not necessary for the wireless access point 112 to perform encryption, because encryption is already being performed by the SB server 102 and the client computer 114A, and neither will transmit plaintext information to the other during the remainder of the session. Once authentication has been performed and the client computer 114A has been given an address for access to the wired network, the client computer 114A is allowed access to network resources according to the privileges associated with the username used in authentication.

It is also possible to employ an SB server to provide connection to a wireless network comprising a plurality of wireless network access points. Providing a plurality of wireless network access points allows users to "roam" from one access point to another seamlessly. The present invention allows a user to authenticate one time and receive a single session encryption key valid at all access points. Fig. 2 illustrates a wired network 200 employing an SB server 202 to provide authentication and security for wireless clients according to the present invention. The wired network 200 also includes a wired network hub 204 and various additional network resources a user database 206 and a DHCP server 208. The SB server 202 provides connection services to allow clients connected to a wireless network 210 to gain access to network resources using the same protocols described above in connection with Fig. 1. The wired network 210 comprises two wireless access points 212 and 214 connected to a network hub 216, which is in turn connected to the SB server 202. The wireless access point 212 is connected to a client computer 218 by means of a wireless network card 220 and the wireless access point 214 is connected to a client computer 222 by means of a wireless network card 224. For simplicity, the wireless network 210 is shown here as comprising two wireless access points, each connected to a single client computer. However, it will be recognized that the wireless network 210 may include any number of wireless access points, each connected to a plurality of client computers, with the only limitation on the number of wireless access points and the number of client computers connected to each access point being those suggested by sound network management practices. Authentication and communication security are preferably performed as described above in connection with the SB server 102 of Fig. 1.

The use of an SB server to control access to a wired network by a wireless network provides good scaling for any size of wireless network. The number of connections to the wired network scales arithmetically as the size of the wireless network increases, with no more than one connection to the SB server being presented with each addition of a wireless access point to the wireless network. Moreover, the management of passwords and keys is not increased in complexity by the addition of wireless access points. When a user leaves a network such as the wired network 200, his or her authorization to use the wired network 200 can be removed at the user database 206, without any need to make changes at any of the wireless network access points such as the access points 214 and 216 in the case of the wireless network 210, or potentially many more access points in the case of a larger network.

Because the radio footprint of a wireless network such as the network 210 is unknown, it must be assumed that an attacker may have access to the radio transmissions used to transfer data between the elements of the network. The attacker may be able to eavesdrop on wireless network sessions, hijack a session by impersonating a client computer with an already established connection to the network, interrupt a session or initiate a session. However, because the wireless network 210 contains no information or access to resources having value to an attacker, the vulnerability of the wireless network is unimportant. Because the wired network 200 is protected by the SB server 202, which implements a well tested authentication system and uses strong encryption to pass data to the wireless network 210, the vulnerability of the wireless network 210 does not compromise any data or resources in the wired network 200. Traffic analysis of the clients and encrypted sessions are available to an eavesdropper, because the communications are radiated over a footprint of unknown size. However, the use of PPTP encapsulates the network traffic, causing all traffic to have an address tuple of the client system and the SB server 202. Traffic analysis, therefore, will not yield the addresses of the SB server and the client computers such as the computer 218.

Fig. 3 illustrates a process 300 of authenticating and securing a connection between a wireless network client and a wired network according to the present invention. At step 302, a connection is established between a wired network and a wireless network. The wireless network may suitably be similar to the wireless network 104 of Fig. 1 and the wired network may suitably be similar to the wired network 100 of Fig. 1. Connection may suitably be estalbished between the wired network and the wireless network by establishing a connection between an SB server similar to the SB server 102 of Fig. 1 and a wireless network access point similar to the access point 118 of Fig. 1. At step 304, a connection is established between a wireless network client and the wireless network, suitably by establishing a connection between the wireless network client and the wireless network access point. The wireless network client may suitably be similar to the computer 114A of Fig. 1, and may suitably communicate with the access point with a wireless network card similar to the network card 116A of Fig. 1. At step 305, in response to a request to establish a connection between the wireless network client and the wired network, encryption keys are exchanged between the wireless network client and the server in order to protect data to be used for authentication. Next, at step 306, authentication is performed for the wireless network client, suitably by requesting and receiving a username and password and comparing the username and password against a user database. The information exchanged between the server and the client is encrypted using the keys exchanged at step 305. If authentication fails, the process proceeds to step 350, the connection is rejected and the connection attempt is logged. If authentication passes, the process proceeds to step 308 and the connection attempt is logged. Next, at step 312, the wireless network client is provided with a temporary address on the wired network, preferably using DHCP, and a unique session encryption key for use in communicating with the wired network. At step 314, traffic is passed between the wireless network client and the wired network through the SB server, with access to network resources being given to the client in accordance with the user privileges associated with the account information provided for authentication.

While the present invention is disclosed in the context of a presently preferred embodiment, it will be recognized that a wide variety of implementations may be employed by persons of ordinary skill in the art consistent with the above discussion and the claims which follow below.

We claim:

1. A wired network for providing secure, authenticated access to wireless network clients, comprising:

a server connected to a wireless network access point, the server being operative to perform authentication for wireless clients establishing a connection to the server through the wireless network access point, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client, the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client; and

a user database accessible to the server for use in validating wireless clients.

2. The wired network according to claim 1 and also including a network hub providing connections between the server and additional resources on the wired network.

3. The wired network according to claim 2 wherein the server is operative to provide addresses to clients through dynamic host control protocol.

4. The wired network according to claim 3 wherein the server is operative to communicate with the wireless network access point using point to point tunneling protocol.

5. The wired network according to claim 4 wherein the server employs 128-bit cryptoprocessing to communicate with the wireless network access point.

6. A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:

a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network, the wireless network access point being operative to conduct encrypted communications with the server, the wireless network access point being further operative to receive authentication information from clients and transfer the authentication information to the server and to receive a cryptoprocessing key from the server and transfer the key to each of the clients; and

a plurality of wireless network clients operative to establish connections with the wireless network access point, each client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point and receive address information and cryptoprocessing data from the network access point to allow communication with the wired network, each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information.

7. The wireless network of claim 6 wherein the access point communicates with the server using point to point tunneling protocol.

8. The wireless network of claim 7, also including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and the additional network access points being operative to establish connections with the server through the network hub.

9. A method of secure communication between wireless network clients and a wired network, comprising the steps of:

establishing a connection between an SB server connected to the wired network and a wireless network access point;

establishing a connection between the SB server and a network client communicating with the SB server through the wireless network access point;

exchanging encryption keys between the SB server and the wireless network client;

performing authentication for the wireless network client;

if authentication fails, rejecting connection to the wired network; and

if authentication passes, accepting connection to the wired network, providing a temporary wired network address and a unique session encryption key to the wireless network client and providing access to wired network resources in response to requests by the wireless network client.

10. The method of claim 9 wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection and wherein the step of accepting the connection is accompanied by a step of logging the acceptance.

ABSTRACT

Techniques for secure connections between wireless network clients and wired network resources are described. An insecure wireless network comprising a plurality of wireless access points provides a connection for wireless network clients to a wired network server which in turn provides controlled access to a wired network. When a wireless network user wishes to connect to the wired network, the user provides authentication information to the wired network server through the wireless network client and the wireless network access point. Once the wired network server has verified the authentication information, the wired network server provides the wireless network client with a temporary wired network address as well as a unique session encryption key, which is used to encrypt all data transferred between the wireless network client and the wired network server during a connection session.

EXHIBIT D

Joe Agusta

From: "steve branigan" <sb@lumeta.com>
To: "Lowell Ross" <lowellross@mediaone.net>
Sent: Wednesday, December 20, 2000 4:17 PM
Subject: Re: Questions

Hello Lowell,
- SB stands for Security Base.
- SSH stands for secure shell. SSH provides secure FTP, Telnet,
and X-windows access. SSH can be used in place of PPTP for
the UNIX/X-Windows environment.
- My address is correct.
- So is Wiliam's

-sb

At 02:31 PM 12/19/2000 -0800, you wrote:
>Dear Steve:
>
>I just have a couple of questions:
>
>What does the SB in SB server stand for?
>
>What does SSH mean? (As in, SSH may be used instead of PPTP).
>
>Is your address 58 Silvercrest Drive, Tinton Falls, NJ 07712, in Monmouth
>County?
>
>What is your middle name?
>
>Is Bill Cheswick's address 93 Mine Mount Road, Bernardsville, NJ 07924, in
>Somerset County?
>
>Thanks!
>
>Lowell
>(714)979-0576

Steven Branigan
VP of Engineering and Co-founder (...and interim CEO)
Lumeta Corp. http://www.lumeta.com
sb@lumeta.com
(908)582-7664

ꜰACSIMILE TRANSMISSION

LAW OFFICES OF PETER H. PRIEST
529 Dogwood Drive
Chapel Hill, N.C. 27516

EXHIBIT E

Telephone : (919) 942-1434

Facsimile : (919) 969-7844
email : phpriest@msn.com

PRIVILEGED AND CONFIDENTIAL: This communication is intended only for the use of the addressee(s) named below and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient(s), please note that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this facsimile in error, please notify us immediately by telephone (collect), and return the original message to us at the above address via the U.S. Postal Service. Thank you.

DATE:	December 21, 2000
TO:	Kenneth M. Brown, Esq.
FIRM:	Lucent Technologies Inc.
FAX NO:	908-582-3859
FROM:	Peter H. Priest
NO. OF PAGES:	24

NOTE: If transmission is poor, or you do not receive all pages, please call (919) 942-1434 as soon as possible.

MESSAGE:

LAW OFFICES OF PETER H. PRIEST, PLLC

529 DOGWOOD DRIVE
CHAPEL HILL, NORTH CAROLINA 27516-2807

919-942-1434
FACSIMILE (919) 969-7844
email phpriest@msn.com

PETER H. PRIEST
LOWELL W. ROSS*
DANIEL KIM*
STEVEN R. QUINLEY

*NOT ADMITTED IN NORTH CAROLINA

December 21, 2000

2412

Kenneth M. Brown, Esq.
Lucent Technologies Inc.
Room 3B-519
600 Mountain Avenue
Murray Hill, New Jersey 07974

Via Facsimile

Re: IDS 121218, Inventors Branigan and Cheswick entitled "Methods and Apparatus for Secure Wireless Networking"

Dear Ken:

Enclosed for your review is the final draft of the above identified patent application. I look forward to your comments.

Very truly yours,

Peter H. Priest

PHP/mmt
Enclosures

PRIEST & GOLDSTEIN, PLLC
529 DOGWOOD DRIVE
CHAPEL HILL, NORTH CAROLINA 27516-2807
919-942-1434
FACSIMILE 919-969-7844
EMAIL phpriest@msn.com

PETER H. PRIEST
RONALD B. GOLDSTEIN*
LOWELL W. ROSS*
DANIEL KIM*
STEVEN R. QUINLEY

* NOT ADMITTED IN NC

NEW JERSEY OFFICE
18 LAKE DRIVE
NORTH BRUNSWICK, NEW JERSEY 08902
732-821-8298
FACSIMILE 732-821-0468
EMAIL rgoldstein@priestgoldstein.com

EXHIBIT F

January 2, 2001

2412

Mr. Steven Branigan
Lucent Technologies Inc.
Room 2T-404
600-700 Mountain Avenue
P.O. Box 636
Murray Hill, NJ 07974-0636

Via Federal Express

Re: Methods and Apparatus for Secure Wireless Networking

Dear Mr. Branigan:

Enclosed are the Declaration and Power of Attorney and Assignment for the above identified case. Please execute these documents at your earliest convenience and return to us for filing in the Patent Office. Note that the Assignment must be executed by a Notary. Please also obtain the signature of William Roberts Cheswick before returning the documents to us. For your convenience we are enclosing a prepaid Express Mail envelope. Thank you for your assistance.

Very truly yours,

Tlynthia P. Jordan
Legal Assistant

tpj
Enclosures

EF 000855747 US

EXHIBIT G

ASSIGNMENT AND AGREEMENT

For value received, we, Steven Branigan of Tinton Falls in the County of Monmouth and State of New Jersey, and William Roberts Cheswick of Bernardsville in the County of Somerset and State of New Jersey, hereby sell, assign and transfer to Lucent Technologies Inc., a corporation of the State of Delaware, having an office at 600 Mountain Avenue, Murray Hill, New Jersey 07974-0636, U.S.A., and its successors, assigns and legal representatives, the entire right, title and interest, for the United States of America, in and to certain inventions related to **METHODS AND APPARATUS FOR SECURE WIRELESS NETWORKING** described in an application for Letters Patent of the United States, executed by us of even date herewith, and all the rights and privileges in said application and under any and all Letters Patent that may be granted in the United States for said inventions; and we also concurrently hereby sell, assign and transfer to Lucent Technologies Inc. the entire right, title and interest in and to said inventions for all countries foreign to the United States, including all rights of priority arising from the application aforesaid, and all the rights and privileges under any and all forms of protection, including Letters Patent, that may be granted in said countries foreign to the United States for said inventions.

We authorize Lucent Technologies Inc. to make application for such protection in its own name and maintain such protection in any and all countries foreign to the United States, and to invoke and claim for any application for patent or other form of protection for said inventions, without further authorization from me, any and all benefits, including the right of priority provided by any and all treaties, conventions, or agreements.

We hereby consent that a copy of this assignment shall be deemed a full legal and formal equivalent of any document which may be required in any country in proof of the right of Lucent Technologies Inc. to apply for patent or other form of protection for said inventions and to claim the aforesaid benefit of the right of priority.

We request that any and all patents for said inventions be issued to Lucent Technologies Inc. in the United States and in all countries foreign to the United States, or to such nominees as Lucent Technologies Inc. may designate.

We agree that, when requested, we shall, without charge to Lucent Technologies Inc. but at its expense, sign all papers, and do all acts which may be necessary, desirable or convenient in connection with said applications, patents, or other forms of protection.

Steven Branigan

Date: 03-jan-2001

United States of America)

State of New Jersey) ss.:

County of Union)

On this 3rd day of January, ~~2000~~ 2001, before me personally came Steven Branigan, to me known to be the individual described in and who executed the foregoing instrument, and acknowledged execution of the same.

MARGARET RAO
Notary Public of New Jersey
Registered in Middlesex County
My Commission Expires August 2, 2001

Margaret Rao

Notary Public

William Roberts Cheswick

Date: 3 Jan 2001

United States of America)

State of New Jersey) ss.:

County of Union)

On this 3rd day of January, ~~2000~~ 2001, before me personally came William Roberts Cheswick, to me known to be the individual described in and who executed the foregoing instrument, and acknowledged execution of the same.

MARGARET RAO
Notary Public of New Jersey
Registered in Middlesex County
My Commission Expires August 2, 2001

Margaret Rao

Notary Public

Lucent Technologies Inc.
600 Mountain Avenue (Room 3C-512)
P. O. Box 636
Murray Hill, New Jersey 07974-0636

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

Declaration and Power of Attorney

As the below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I hereby claim the benefit under Title 35, United States Code, 119(e) of any United States provisional application(s) identified below:

None

I believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHODS AND APPARATUS FOR SECURE WIRELESS NETWORKING**, the specification of which is attached hereto.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by an amendment, if any, specifically referred to in this oath or declaration.

I acknowledge the duty to disclose all information known to me which is material to patentability as defined in Title 37, Code of Federal Regulations, 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

None

I hereby claim the benefit under Title 35, United States Code, 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

None

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

I hereby appoint the following attorney(s) with full power of substitution and revocation, to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected therewith:

Thomas J. Bean	(Reg. No. 44528)
Lester H. Birnbaum	(Reg. No. 25830)
Richard J. Botos	(Reg. No. 32016)
Jeffery J. Brosemer	(Reg. No. 36096)
Kenneth M. Brown	(Reg. No. 37590)
Donald P. Dinella	(Reg. No. 39961)
Guy Eriksen	(Reg. No. 41736)
Martin I. Finston	(Reg. No. 31613)
William S. Francos	(Reg. No. 38456)
Barry H. Freedman	(Reg. No. 26166)
Julio A. Garceran	(Reg. No. 37138)
Jimmy Goo	(Reg. No. 36528)
Anthony Grillo	(Reg. No. 36535)
Stephen M. Gurey	(Reg. No. 27336)
John M. Harman	(Reg. No. 38173)
Matthew J. Hodulik	(Reg. No. 36164)
Michael B. Johannesen	(Reg. No. 35557)
Mark A. Kurisko	(Reg. No. 38944)
Irena Lager	(Reg. No. 39260)
John B. MacIntyre	(Reg. No. 41170)
Christopher N. Malvone	(Reg. No. 34866)
Scott W. McLellan	(Reg. No. 30776)
Martin G. Meder	(Reg. No. 34674)
John C. Moran	(Reg. No. 30782)
Michael A. Morra	(Reg. No. 28975)
Gregory J. Murgia	(Reg. No. 41209)
Claude R. Narcisse	(Reg. No. 38979)
Joseph J. Opalach	(Reg. No. 36229)
Neil R. Ormos	(Reg. No. 35309)
Eugen E. Pacher	(Reg. No. 29964)
Jack R. Penrod	(Reg. No. 31864)
Gregory C. Ranieri	(Reg. No. 29695)
Scott J. Rittman	(Reg. No. 39010)
Ferdinand M. Romano	(Reg. No. 32752)
Eugene J. Rosenthal	(Reg. No. 36658)
Bruce S. Schneider	(Reg. No. 27949)
Ronald D. Slusky	(Reg. No. 26585)
David L. Smith	(Reg. No. 30592)
Ozer M. N. Teitelbaum	(Reg. No. 36698)
John P. Veschi	(Reg. No. 39058)

David Volejnicek	(Reg. No. 29355)
Charles L. Warren	(Reg. No. 27407)
Jeffrey M. Weinick	(Reg. No. 36304)
Eli Weiss	(Reg. No. 17765)

I hereby appoint the attorney(s) on ATTACHMENT A as associate attorney(s) in the aforementioned application, with full power solely to prosecute said application, to make alterations and amendments therein, to receive the patent, and to transact all business in the Patent and Trademark Office connected with the prosecution of said application. No other powers are granted to such associate attorney(s) and such associate attorney(s) are specifically denied any power of substitution or revocation.

Full name of 1st joint inventor: Steven Branigan

Inventor's signature ______________________ Date 1/3/01

Residence: Tinton Falls, New Jersey

Citizenship: USA

Post Office Address: 58 Silvercrest Drive, Tinton Falls, NJ 07712

Full name of 2nd joint inventor: William Roberts Cheswick

Inventor's signature ______________________ Date 3 Jan 2001

Residence: Bernardsville, New Jersey

Citizenship: USA

Post Office Address: 93 Mine Mount Road, Bernardsville, NJ 07924

ATTACHMENT A

Attorney Name(s): Peter H. Priest Reg. No.: 30,210

Telephone calls should be made to **Peter H. Priest** at:

Phone No.: (919)942-1434

Fax No.: (919)969-7844

All written communications are to be addressed to:

Peter H. Priest
Law Offices of Peter H. Priest, PLLC
529 Dogwood Drive
Chapel Hill, NC 27516